



CONNECT

CONNECTING OUR CLIENTS THROUGH KNOWLEDGE

ARE FINANCIAL SERVICES COMPANIES HEADING FOR TOUGH DECISIONS AS WE EMERGE FROM THE PANDEMIC?



IS APP FRAUD AND PAYEE AUTHENTICATION LIKELY TO BE THE MOST PRESSING ISSUE IN 2021?

BUILDING AN EFFECTIVE CBIL/BBLs FRAUD RISK AND RECOVERY STRATEGY WITH SYNECTICS

HOW ARE FINANCIAL CRIMINALS USING COVID-19 TO ADAPT THEIR OPERATIONS?

03 Your Latest Releases

Update on the latest functionality that we're releasing to SIRA clients to help improve their ability to mitigate fraud and other financial crime risks.

04 ENHANCEMENTS TO REAL-TIME QUOTES CREATES UPLIFT IN FRAUD IDENTIFICATION

Adding new data items to the ruleset enables commercial policy screening opportunities for RTQ.

08 Building an effective Coronavirus Business Interruption Loan or Bounce Bank Loan Scheme (CBIL/BBLS) Recovery Strategy.

10 Fraud Trends

How has the pandemic affected patterns of fraud amongst Synectics clients - And how have some clients adapted their business to address the new normal?



14 Vulnerability Registration Services, Helen Lord: Achieving greater protection for vulnerable customers thanks to Synectics partnership with the VRS.

16 Yoti

Gareth Narinesingh highlights the increased need for financial services companies to expedite their digital on-boarding capabilities as face-to-face customer interaction becomes a distant memory.

18 How are financial criminals using COVID-19 to adapt their operations?

Peter Taylor, Financial Crime Consultant, uses his inside knowledge to examine how criminals have adapted their activities and are preparing to exploit the new vulnerabilities that have emerged during these last few months.

20 HAS APP FRAUD AND PAYEE AUTHENTICATION BECOME ONE OF THE MOST PRESSING CHALLENGES IN 2020 FOR FRAUD TEAMS?

22 Upcoming events

Throughout the year we're hosting a series of webinars, client events and thematic calls. Make sure you have the dates in your diary!

06 ARE FINANCIAL SERVICES COMPANIES HEADING FOR TOUGH DECISIONS AS WE EMERGE FROM THE PANDEMIC?

As government support schemes come to end, are your financial crime defences ready for a post pandemic world?



MESSAGE FROM
Katy Worobec
MANAGING DIRECTOR,
ECONOMIC CRIME - UK FINANCE

The 16th March 2020 seems like a long time ago as the point at which the UK went into lockdown. Despite all the clichés about 'unprecedented times' our financial services sector has risen to the challenge of keeping the UK economy afloat in these turbulent times.

Despite all the logistical and operational issues that the COVID-19 pandemic has thrown our way, in conjunction with the UK Government our industry has proven a level of resilience that quite simply wouldn't have been possible if it wasn't for the transformation that has taken place in the sector since the 2008 financial crisis. In particular, the industry came together with government, law enforcement and other sectors quickly to tackle emerging attacks from those exploiting the COVID-19 crisis - in one example, working with text message providers and law enforcement to block scam text messages from unauthorised sender IDs mimicking trusted organisations.

However, as we emerge from this pandemic further challenges lie ahead, and we must all reflect on the 'lessons learned' of how our various organisational structures have adapted to the new normal - and assess what further changes need to be made to ensure stability, success and growth for the longer term.

The economic climate that is likely to emerge from this crisis for some time is going to be one of low interest rates and low profitability for many. Despite this the risks from vulnerable economies and customers also means banks, insurers and other finance providers must remain vigilant and responsive to the likely growth in regulatory compliance challenges and the fraud and financial crime risks that will parallel those economic realities.

Despite these conditions, I am certain that with the correct focus and innovation, there are still tremendous opportunities to transform the way in which we address these risks through the better use of technology and a willingness by all of us to adopt a more collaborative approach to sharing intelligence and best practice - both between organisations and with UK regulators/law enforcement.

The likelihood is that those who embrace and implement this transformation to create better customer experiences - and increase the efficiency and resilience of their organisations - will emerge from this in good shape for the new realities we face going forwards.

NEW FUNCTIONALITY YOUR LATEST SIRA RELEASE



SQL WEB TOOL - UPGRADE

Analysing adverse data from within your SIRA implementation has now become easier thanks to an improved user interface and some key bits of new functionality. The new functions within SQL Web Tool include;

- The text editor now displays SQL Syntax, making SQL query writing much easier and user friendly
- There is now an Auto Complete function when picking table names & generic SQL functions when writing your data queries, which will speed up your query writing and help to prompt for those difficult to remember table names when trying to pull data for reports
- We have also added buttons to clear old SQL queries & hide unused tools from your view to make writing queries simpler



CASE HISTORY NOTES WIDGET - CLICK TO EXPAND FEATURE

To improve the user interface of the Case Notes History widget in SIRA, we've made it possible to expand the view of the notes you have made against cases at the click of a mouse - so you can click to expand or collapse your notes. We've done this to make your ability to access useful case data easier without getting in the way of analysing matching data when reviewing cases.



REMOVED INVALID CHARACTERS FROM DATA LOADING PROCESSES

To make the whole loading process of data into SIRA batch feeds more resilient, and reduce loading errors, we've enhanced the range of character exclusions. This will reduce the amount of failures seen when calling 3rd party data services to improve the overall success rate of returning information to be used in rules and to be displayed to SIRA users. For more details on the character exclusions you will find these in your latest SIRA members Release Note - R3 2020.



For more information...
on how to access these upgrades please get in touch with your SIRA Customer Success Manager in the first instance.

IMPROVEMENTS IN SIRA'S RTQ (REAL-TIME QUOTE) SOLUTION RULE SET GETS AWARD NOMINATION FOR ALLIANZ AT INSURANCE TIMES AWARDS

+ SIRA'S RTQ SERVICE CAN NOW BE USED TO FRAUD SCREEN COMMERCIAL POLICY UNDERWRITING

+ ENHANCED SCREENING DATA CREATES 9% UPLIFT IN IDENTIFICATION OF FRAUD AT POINT OF QUOTE

SIRA's Real-Time Quote (RTQ) solution has been providing members of the National SIRA community with the ability to screen policy applications at 'point of quote' for over 6 years. Clients using RTQ have reported being able to reduce their post app fraud referral rates by as much as 20%, which equates to huge savings in reduced investigation/administration costs.

At the same time, RTQ provides the ability to reduce the risks of onboarding 'bad-business' much earlier in the customer journey thereby further protecting companies from losses to fraud.

To enhance the capabilities of the RTQ solution, we have improved the range of data items that can be incorporated into the rule engine to make it even more effective at identifying fraud - while also opening up commercial insurance as a sector that can make use of the service.

REDUCE POST APP FRAUD REFERRAL RATES BY AS MUCH AS

20%



As part of this work, we've added in the ability to include 'Email Address' and 'Telephone' data items into RTQ's rule set to help clients improve and refine RTQ's fraud rules.

BY ENHANCING RTQ RULESET TO INCORPORATE SOME OF THESE NEW DATA ITEMS CREATED A



9% UPLIFT
IN ADVERSE POLICY IDENTIFICATION

A recent Proof of Concept (PoC) with an RTQ client showed that by enhancing their RTQ ruleset to incorporate some of these new data items created a 9% uplift in their adverse policy identification from the previous implemented ruleset.

Markerstudy have been a user of RTQ for some time and Craig Lawrence, Head of Technical Services at Markerstudy said the following about how effective RTQ had been for their business;



“

Before we had the SIRA RTQ capability we were being severely hampered by "Repeat Offender" fraud cases. These were risks we had identified, investigated and ultimately removed from cover in line with CIDRA. However, there was little to prevent the same PH coming straight back on cover through our various channels. In one case, we saw the same risk 43 times! The RTQ rules meant we were able to ensure that this was no longer possible - subject to an Inconsistent, Fraud or High Risk status set on SIRA. The positive impact of SIRA RTQ on resource was significant, not to mention the uplift in morale of the team who were no longer having to continually repeat the process on the same entity. In addition, using the system to filter out additional fraud before it comes on the books has provided our teams the opportunity to proactively find the fraud in other areas, build new strategies accordingly to further reduce our fraud exposure.

"SIRA RTQ is a great example of technology working for the business, and ultimately its customers, to reduce the cost of fraud."


CRAIG LAWRENCE, HEAD OF TECHNICAL SERVICES

 **IMPROVE**
YOUR FRAUD DEFENCE WITH SIRA RTQ

 **REDUCE**
YOUR INVESTIGATION RESOURCE COSTS

ENHANCED RULE SET CREATES FURTHER **9% UPLIFT IN FRAUD IDENTIFICATION** 

 ABILITY TO PROCESS IN EXCESS OF **4 MILLION QUOTES PER DAY**

 **MITIGATE THE LIKELIHOOD OF BOARDING FRAUDULENT BUSINESS**

SUB 3 SECOND RESPONSE TIME  PER APPLICATION

SCREEN YOUR APPS AGAINST THE ENTIRE NATIONAL SIRA DATABASE

NOW ABLE TO SCREEN FOR COMMERCIAL POLICIES 

Both new and existing SIRA clients can take advantage of the improvements and if you would like to explore the benefits of improving your ability to reduce fraud at 'point of quote' then please do get in touch with your Client Success Manager at Synectics or **call 0333 234 2414 and ask to speak to Chris Hallett.**

ARE FINANCIAL SERVICES COMPANIES HEADING FOR

TOUGH DECISIONS

AS WE EMERGE FROM THE PANDEMIC?



Having steadied the ship during the COVID-19 pandemic after one of the most severe crises in living memory, the global financial services industry has, for a number of weeks now, been shifting gear from firefighting to properly addressing what is transpiring into the new normal.

No organisations have been untouched and all businesses are having to make some very tough decisions on a number of fronts as they get to grips with the state of the economies in which they are operating. In addition to short term adjustments longer-term responses will be dictated by the perception of what kind of national or global recovery we are likely to see.

At the early stage of the pandemic, optimists were predicting a rapid 'V' shape bounce-back to normality. However, as this crisis has continued there has been a reality check occurring as we witness countries all over the world stumbling back into various forms of restricted living and lockdown as the virus re-emerges into communities.

A recent piece of research by McKinsey amongst 2000 global executives in the banking sector pointed to expectations of a slow economic recovery and patchy growth at best. These executives all agreed on two scenarios for financial service providers; credit losses will be substantial, and income from interest is going to be significantly depressed for the foreseeable future. So there is going to be a double squeeze on profitability just at a time when these organisations need to make some significant investment decisions to ensure the fitness of their business to remain competitive.

Faced with this reality, banks, insurers and others are all having to recalibrate the impact of the economic and behavioural changes that have occurred as a result of the pandemic on their customers' lives - as well as the changes that will have to occur within their own organisations.

Tough decisions around the shape and size of their future workforces have already been some of the initial choices, as media reports have widely reported various redundancy decisions being taken. In the UK alone 100,000 jobs are reported to have gone or being at risk in the banking sector.

However, from a financial crime risk perspective the considerations are going to be very wide ranging and impact a range of areas within the businesses concerned. Heightened risks around bad-debt, fraud and increased customer vulnerabilities are going to be paramount over the next few years.

Absence of face-to-face contact increases the need to prioritise digital onboarding capability that's fit for purpose

From a commercial perspective, the evaporation of traditional 'face-to-face' routes to market has meant that truly digital methods of identifying and onboarding customers have had to be reassessed and reprioritised to ensure that they are fit for purpose.

Do the current platforms on offer provide the quality of customer experience required to be competitive - more importantly are they capable of properly assessing customer risk without causing too much friction on the sales process?

The increased opportunities presented to financial criminals in the new normal

The prevalence of home working, now so common and likely to remain in place for some time, also has a double impact on financial crime and fraud risk teams responsible for protecting their businesses.

Not only does the prospect of increased numbers of customers working from home give fraudsters and cyber criminals much more opportunity - through the use of malware or social engineering tactics (such as posing as company help-desk teams) - but they will also need to consider the risk factors of their own workforce conducting business in this distributed/remote environment.

Additionally, as we have reported elsewhere in Connect, the increased levels of economic vulnerability of local populations is going to make the temptation of external fraud more prevalent amongst customers under financial distress - not to mention the fertile ground this offers for organised crime groups to exploit.

So faced with this environment, what are some of the areas that need to be prioritised from a fraud and financial crime transformation perspective?

Broadening your access to external intelligence

Banks, insurers and other finance providers would be advised to increase their ability to develop a more rounded view of risk. This can be achieved through a re-evaluation of the various data partners you work with to ensure that you have the necessary external intelligence to understand the external environment as things evolve in real-time.

Linking external intelligence to internal customer knowledge

Having the ability to link external intelligence to internal customer data to create a unified, 360-degree, view of the risks that customers pose will be essential to reduce the likelihood of exposing the business to financial crime - but also to improve your ability to treat vulnerable customers with a greater degree of fairness in what looks like being difficult times ahead.

Improving your use of advanced analytics

Reduced levels of resource, exponential increases in the volume of inbound referrals, increased regulatory screening commitments, and the demands of instant decision making can paralyse a fraud or financial crime team. Taking advantage of the various analytic techniques that have become available can transform your ability to create a decision platform that can accommodate a real-time decision environment, without compromising the financial crime mitigation or compliance processes you need to satisfy.

Machine learning, predictive analysis and various other forms of sophisticated link analysis can all enable the automation and speeding up of decision making without compromising risk mitigation and compliance measures that are required.

Centralising disparate financial crime intelligence and teams

The legacy of mergers that took place post 2008 has meant that many organisations have a complex web of fraud and financial crime risk decision making units that are uncoordinated and disconnected. This creates a huge burden on those looking to reduce the cost of customer acquisition while simultaneously trying to speed up the ability to 'green-light' applications and get products out to market. Creating a truly unified risk platform that unites the various disparate teams in the organisation and allows them to make effective real-time risk assessments will be essential. This will help to reduce costs and the likelihood of duplication or costly mistakes being made from a lack of data quality.

Increasing collaborative efforts to mitigate risk within and across vertical markets

Criminals of all stripes are often repeat offenders and will have left a footprint that organisations can use to ensure they are not their next victim. Collaborative intelligence sources, such as National SIRA, CIFAS, CUE, or the UK Government's NFI, have proved incredibly successful at helping companies to mitigate their exposure to fraud and financial crime. More recently opportunities to use Public Sector intelligence sources (in the UK) to help enrich data and identify fraud or other types of financial crime have also become available to use. The financial sector needs to continue to embrace the spirit of cooperation and collaboration in this regard to improve their defences.

Additionally many types of analysis techniques being deployed to block adverse business have been modelled on shared industry intelligence sources - and so it's vital for these resources to be maintained so as to ensure that these techniques do not become inoperable.



Ultimately, there will be certain characteristics of financial services organisations that are able to succeed in the new world that emerges from the COVID-19 pandemic. Those who are able to successfully digitise customer interactions, restructure their operations while simultaneously evolving their value propositions to respond to rapidly changing customer needs will be the victors.

Those who lack the will and ambition to take some of the key decisions to transform their business might find themselves struggling to compete in the choppy waters that lie ahead.

BUILDING AN EFFECTIVE CORONAVIRUS BUSINESS INTERRUPTION LOAN OR BOUNCE BANK LOAN SCHEME (CBIL/BBLS) RECOVERY STRATEGY

Dealing with the CBIL/BBLS loans as part of the various COVID-19 recovery operations has left many banks wondering how to go about creating a process that enables them to meet their recovery commitments without derailing other important due diligence or customer risk assessment activities.

Chris Lewis, Head of Pre Sales at Synectics, outlined a strategy for an effective CBIL/BBLS recovery strategy in a recent article using third party intelligence sources accessible within Synectics Data Marketplace to deal with the challenges effectively.

A summary of his thoughts can be found in this article -

TO READ THE FULL ARTICLE CLICK HERE →

“ The speed at which the Coronavirus Business Interruption Loans Scheme (CBILS) was deployed to ensure UK business stability, at what was probably the most precarious time for British business since the end of World War II, has been a testament to the agility, commitment and professionalism of the UK banking industry. However, as the COVID-19 pandemic unfolds those businesses who have taken out these government backed loans will have to consider a sensible repayment strategy as we emerge from this crisis and they begin trading again. While the UK Government has agreed to underwrite the majority of the loans, financial institutions who have awarded CBILS and Business Bounce-back Loans (BBLS) will still be expected to make efforts to recover them where appropriate.”

RISK FACTORS

Fraud checks were one of the few measures included within the BBLS scheme as it was rolled out.

In fact, Synectics' collaborative fraud intelligence database (National SIRA) has been at the heart of the measures in place to help with that and was a resource specifically mentioned within the UK Government's legislation accompanying the BBLS and CBILS schemes.

As a result, Synectics have already processed a large proportion of these loans and are able to easily identify incidences of fraud, where a business may have successfully applied for multiple loans with multiple lenders.

However, to create a more effective collection strategy for these loans, and one that goes beyond just a simple fraud check, we would advise analysing a wider set of risk factors to create a much more intelligent recovery strategy that will help to better prioritise cases that require investigation or recovery - and avoids a costly and ineffective 'one size fits all' approach to your collections processes.



Trading Status
was the business trading prior to lockdown and has the business begun trading again?



Affordability
is there financial information available about the business to assess affordability and repayment?



Geographic Area
is the business located in an area which was already struggling prior to the lockdown, and how is this area recovering in comparison to the national average?



Sector Health
is the business in a high risk sector (leisure, retail, hospitality, etc.?)



Key Personnel
are there any characteristics about key personnel related to the business (directors, board members, etc.) that indicate poor financial health and/or potential to commit fraudulent activity?

HOLISTIC VIEW 1

Following the identification of the risk factors, the aggregation and analysis of various proprietary, public and third party data sources can create a much more holistic view of risk associated with each business that has used any of the loan schemes.

Ultimately this will provide lenders with actionable intelligence to enable them to finesse their collection strategies and prioritise efforts for recovery much more effectively. This will save significant time and resource in targeting collections and recovery investigations where they are most appropriate.

Synectics recommend an approach that encompasses a range of intelligence sources to achieve this kind of process such as:

Fraud consortium data (National SIRA & CIFAS)

assessing the fraud risk associated with both the business and key personnel, whilst identifying potential businesses that may have applied for multiple loans.

Public sector data (National Fraud Initiative)

amalgamating publicly available information about businesses (Food Standards Agency, Charities Commission etc.) with public sector fraud data held within the National Fraud Initiative to identify material discrepancies.

Real-time available commercial intelligence

intelligence regarding the historical, current and future trading status of businesses, including geodemographics, vacancy rates, openings and closures activity, company structure, etc.

Credit & affordability checks

financial indicators for both businesses and key personnel to ensure businesses are beginning to recover, including financial information regarding payment holidays, furlough and unemployment indicators.

PRIORITISATION 2

Once this aggregated view of commercial risk is built we would recommend creating a regularly updated matrix that could then provide a much more intelligently prioritised group of customers for the bank to focus their collections strategy on.

This could be achieved by applying a set of business rules to use the intelligence mentioned above to match and rank businesses based on various criteria, reflective of the likelihood of recovery, and subsequent prioritisation of collections activity.

Conversely, there should also be a significant focus on identifying businesses which are not likely to resume trading and ultimately default.

Further analysis could also provide geographic, business sector, or commercial risk analysis depending upon how the remaining effects of this pandemic affect certain sectors and impact their wider credit & affordability issues.

RECOVERY 3

With a strategy, such as the one outlined, a much more targeted and cost-effective process can be put in place focused only those businesses that will be in a position to begin repayment (of both CBILS and BBLS loans) in the next 12-18 months.

Businesses that are unlikely to survive could ultimately be written off, to avoid wasting valuable resources on loans that won't be recovered and will have to be underwritten by HM Treasury.

There should also be a focus on potential fraudulent applications from businesses taking advantage of the scheme via applying through multiple lenders, or multiple organisations from the same corporate structure applying (e.g. individual pubs in a pub chain).

“Businesses that are unlikely to survive could ultimately be written off, to avoid wasting valuable resources on loans that won't be recovered...”

Banks could utilise 3rd party resource on a “pay as you recover” basis to maximise returns in this area, mitigating sunk spend on recovery in this continuing uncertain collections landscape.



Synectics have already processed a large proportion of these loans and are able to easily identify incidences of fraud.”

More information, get in touch with us...

For more information regarding Synectics' initiatives for CBILS & BBLS post-award checks, collections & recoveries please get in touch with Synectics Solutions Consultant, Chris Lewis at chris.lewis@synectics-solutions.com

Latest fraud trends 2020

National SIRA fraud data creates a window into the lives of the UK population during the COVID-19 lockdown

The amount of finance and insurance applications that were submitted to the National SIRA database during the COVID-19 lockdown period (March – July 2020) were understandably reduced (by 19% overall) as the UK population's appetite for various types of financial products and services responded to the conditions imposed on them by the government COVID-19 shutdown.

However, a brief analysis of the patterns of changing submissions by the National SIRA community shines an interesting light on the evolving habits of the UK public, from the perspective of their finance and insurance applications, as they reacted to the new conditions they found themselves in.

Despite retail finance product submissions declining, business loans being submitted to National SIRA (in the form of CBILS/BBLs and traditional business finance screening) increased by a factor 400% at one point as the SIRA community used the tools at their disposal to help mitigate the risk of fraud amongst some of the various government led financial support packages being offered to protect the UK economy in the face of this unprecedented shutdown.

 Business loans being submitted to National SIRA **INCREASED BY A FACTOR 400%**

From an Insurance perspective, as one would expect the amount of Motor Claims being submitted for review dropped by over 25% as the UK population's ability to move around was curtailed by the lockdown conditions. However, unsurprisingly the nation still needed to have sufficient insurance cover in place for their various needs and Policy Applications submitted to SIRA for review were only marginally down (7%) on 2019 levels.

MOTOR CLAIMS SUBMITTED DROPPED BY 25%

The following analysis considers the effects of the UK's Lockdown in more granular detail and reveals some interesting patterns that reflect the nature of COVID-19 as it effected people's lives, as well as indicators of the impact of various UK government economic stimulus measures as the situation evolved.

From a fraud perspective, there were some significant increases in fraudulent activity identified by SIRA members in certain types of financial product that the National SIRA community need to be wary of - which is covered in greater detail below.

TRENDS BY PRODUCT

CREDIT CARDS



40% DECREASE IN CREDIT CARD APPLICATIONS

There was an immediate drop in credit card applications by around 40% in March, which has been maintained as the lockdown continued. As lockdown ended, this gap from 2019 appeared to be narrowing to around 30%.

As a result of the drop in CC applications adverse/fraudulent applications represented the same proportions, in-line with the same ratio that we have seen in 2019.

RETAIL FINANCE



20% DECREASE IN RETAIL FINANCE APPLICATIONS

Retail finance applications were trending down by around 20% prior to the lockdown reflecting the slowdown in the economy that was occurring pre-COVID. However, it seems once people were forced to spend time at home in the lockdown applications rose and increased year on year by around 12% for the 2 months of the 'full-on' lockdown. As movement restrictions eased throughout June/July, it appears people in the UK found things other than online shopping to occupy their time and retail finance again declined back to around 20% down on 2019 levels.

The proportion of adverse or fraudulent applications remained roughly in line with previous years' ratios.

UNSECURED LOANS



90% INCREASE IN THE RATIO OF APPLICATIONS FLAGGED AS FRAUD

Pre-lockdown Unsecured Loan SIRA submissions were trending pretty much in-line with 2019 levels (slightly down by 10%). However, as lockdown took hold, with the immediate panic that ensued, these fell away to reduce by around 35% through March and April. However, as the various UK stimulus measures were released and people were able to understand their own economic circumstances better it seems that volumes recovered slightly - but were still trending around 15-20% lower than 2019.

Interestingly from an adverse/fraud perspective, the ratio of applications flagged as fraud during this period did increase by a staggering 90%. Indicating that despite overall application volumes being down, fraudsters were increasingly trying to take advantage - perhaps because of their perception of bank's having to adapt their resources to the crisis.

TRENDS BY PRODUCT

MORTGAGES



**79% DECREASE
IN MORTGAGE
APPLICATIONS**

Unsurprisingly applications for mortgages fell away and reduced, by as much as 79% at one period in April, as the confidence of UK house-movers evaporated. However, it seems that the UK Government's attempt to stimulate the market by offering the Stamp Duty holiday in June was successful, and National SIRA saw a fairly swift return to 2019 mortgage loading levels by June as confidence returned - and perhaps people took advantage of the government stimulus measures.

From an adverse/fraud perspective, the ratio of applications being submitted that were deemed fraudulent remained identical to 2019 levels.

CURRENT AND SAVINGS ACCOUNTS



**25% INCREASE
IN FRAUDULENT
APPLICATIONS**

Current and Savings accounts being loaded to SIRA for screening took a significant increase from May onwards, with the latter period of lockdown showing volumes up by as much as 27%. Many in the UK, with significant sums in their Current Accounts, are reported to have been trying to open up new locations to deposit money, which may explain the leap in new account openings that occurred.

From a fraud perspective, there was a 25% increase in applications being deemed fraudulent after screening. As we know new bank accounts are a highly effective tools for fraudsters and it seems that those with criminal intent were increasingly attempting to open up new accounts to perpetrate their various activities during this time.

Wider intelligence about organised criminals trying to access various government COVID-19 loans and grants might also play into the need for crime gangs to have been increasingly active in account opening as they sought to 'cash-out' their gains - is a subject covered in further articles in Connect.

BUSINESS LOANS



**400% INCREASE
IN BUSINESS LOANS
BEING SCREENED**

As alluded to in the summary, business loans saw a huge spike in products being screened by SIRA members as banks drew on their various resources to screen the many loans being dealt with (such as CBILS/BBLS) as UK businesses tried to manage the rapid injection of government backed loans into the UK economy. At one point in May, there was a 400% spike in business loans being screened by SIRA in comparison to the previous year.

From a fraud perspective, there doesn't appear to have been a significant increase in cases of applications deemed fraudulent at point of application. However, wider analysis of the various government-backed loans during this time suggests that the impact of fraud in this area probably won't become apparent until such time as loan recovery operations commence.

INSURANCE



**25% DECREASE
IN MOTOR CLAIMS
SUBMITTED
FOR REVIEW**

In terms of trend there were no major shifts in policy submission volumes to the SIRA database as the pandemic unfolded. The only significant occurrence was in the area of Motor Claims, which dropped by over 25%. Hardly surprising considering that the majority of the UK population's opportunity to travel had been put on hold.



**50% INCREASE
IN RATIO OF FRAUD
FOR MOTOR CLAIMS**

When it comes to assessing the fraudulent nature of these products loaded there was a 50% increase in the ratio of adverse/fraudulent Motor Claims identified albeit from a much lower volume of cases submitted for review. Adverse policies were broadly in line with 2019 levels.

SIRA MEMBERS PERSPECTIVE

ON DEALING WITH THE COVID-19 PANDEMIC

CONNECT ASKED TWO OF OUR CLIENTS FOR THEIR PERSPECTIVE ON HOW THEIR RESPECTIVE ORGANISATIONS DEALT WITH THE CHALLENGES THAT THE PANDEMIC PRESENTED THEM WITH FROM A FRAUD AND FINANCIAL CRIME PERSPECTIVE;

**James
Burge**

Allianz

**FRAUD MANAGER,
ALLIANZ**

"The Covid-19 pandemic is affecting just about every aspect of our lives with the insurance sector no exception. As we all know well from history, a crisis and tough economic times invariably means an uptick in insurance fraud, whether it be opportunistic or organised. At Allianz, from the very start of the pandemic, we were in a very fortunate position to have excellent people, processes and tools in place to protecting our genuine customers interest.

"We also had the benefit of being part of a large global organisation and we were able to leverage some great insights. The Allianz Group shares emerging threats and best practice on fraud with other members in its network. Through this, the experiences of Spain and Italy, both of which were further along the curve with the virus, proved to be particularly valuable.

"We have been able to monitor the effects of the pandemic and although so far we have seen a slight reduction in detection levels, we saw very few cases specifically related to covid-19. Throughout this time, we have also been able to review our processes to ensure we maintain effective and efficient journeys for our genuine customers. As the world starts to return to some form of normal, albeit we have now officially entered into a recession, we believe that detection levels will start to increase more than ever. We know that with a recession comes financial strain for both individuals and businesses, so I personally believe that we are at a pivotal moment where we need to brace ourselves for an increase.

"These are challenging times for insurers and their policyholders so it is really important that as an industry we work together and share intelligence to tackle this issue, whilst ensuring we continue to support our genuine customers."

**Simon
May**

Nationwide

**FRAUD ANALYTICS SENIOR MANAGER,
NATIONWIDE**

"Fraud-wise, we saw an initial reduction in activity when the UK's lockdown started. Along with most of us, the fraudsters were in shock and seemed to take some time to regroup. This didn't take long and, once things picked up, the fraud levels have reached levels in excess of what we were seeing pre-Covid-19. We've seen a significant rise in digital banking activity from both fraud and genuine perspectives.

"Smishing has been the main driver of case volume in this area. Remote access cases, where fraudsters use software to remotely control the victim's computer, went very quiet for a couple of months and have gradually picked back up again - this correlates with India's lockdown where call centres were closed temporarily. Investment scams have increased sharply, where fraudsters are taking advantage of low interest rates and financial market volatility to convince victims to send payments for so-called bonds and investment opportunities. Card-present activity plummeted during lockdown and the fraud activity followed a similar pattern, but both genuine and fraudulent card activity migrated to online shopping very quickly and a good proportion of this change in behaviour seems to be persisting, despite lockdown measures easing.

"I think some of the trends we've seen emerging in recent months are likely to continue in the medium term, particularly the rise in digital banking fraud and investment scams. In terms of Authorised Push Payment scams, we will continue to see the shift towards victims' financial providers being liable for losses, forcing the industry to continue to offer greater protection for our customers.

"There are positive signs on the horizon for card-not-present fraud with Strong Customer Authentication being rolled out for online shopping. I expect this to gradually reduce the volume of card-not-present fraud cases but we're likely to see more social engineering MOs emerge, with victims tricked into giving away one-time passcodes.

"A potential downturn in the UK housing market (once the current spike is over) could lead to more mortgage fraud and I would expect to see more broker and solicitor enabled fraud taking place in a slower housing market."



GREATER PROTECTION FOR VULNERABLE CUSTOMERS THANKS TO SYNECTICS PARTNERSHIP WITH THE VRS

The COVID-19 pandemic has rocked the UK's economy, and with it exacerbated the fragility of a large proportion of the UK population's financial stability. Even before the pandemic struck, there was a growing issue with how financial services (FS) companies identify and deal with those who are vulnerable for some time. As we reported in a previous edition of Connect the FCA, as far back as 2015, highlighted that more needed to be done to harmonise the way in which the FS community dealt with financially vulnerable customers.

So, as part of Synectics focus on helping our clients to use shared intelligence to improve how they deal with various risk assessment challenges, we recently signed a partnership agreement with the Vulnerability Registration Service (VRS). This groundbreaking service promises to significantly help FS companies to be much more informed about various types of vulnerability issue, when customers' accounts and transactions are being risk assessed.

Connect asked, **Helen Lord Director at the VRS**, to give us a short update on some of the developments of the VRS service over the last few months;

Can you explain the VRS?

The VRS is a central and independent database notifying organisations when vulnerable people need their circumstances taken into consideration or where applications, made in their names, should be declined. It is a tool to help companies treat people in an appropriate manner, and adds a defence against fraudulent activity, while working to meet the expectations of the FCA.

“Thanks to our partnership with Synectics, clients using Synectics Data Marketplace can access VRS data via an API.”

What have VRS been working on to enhance the database in recent months?

We have recently taken over the provision of the vulnerable data previously held by Cifas. Cifas previously ran the Protecting the Vulnerable service, whereby data was obtained from local authorities, solicitors and estate management companies. This includes information relating to an extremely vulnerable population in the form of Court of Protection Orders, Appointee-ships and Power of Attorneys. VRS has also added flags to highlight where people have fallen into vulnerable circumstances because of the pandemic and where people have accessibility issues e.g. no internet access.

What kind of mechanisms have you been putting in place to allow companies to access this data?

VRS has developed a series of 'sub-flags' in our database to provide additional information where somebody is identified as vulnerable. This is to enable companies to take the right approach when screening their customers. The flags are provided with full customer consent and identify where there is physical disability, mental capacity issue, an impact from life events (such as divorce, bereavement or addiction), or where there is extreme financial difficulty. Our flags have also taken into consideration the views and needs of various FS organisations, regulators, trade associations and stakeholders.

How can FS organisations access this intelligence?

Thanks to our partnership with Synectics, clients using Synectics Data Marketplace can access VRS data via an API. This will allow existing Cifas members to continue to receive the information previously obtained through the Protecting the Vulnerable service plus having the added benefit of the additional information held in the growing VRS database. Non-Cifas members will also be able to access the information

Any clients who would like to understand more about how the VRS data service might help to improve the risk assessment and customer screening of vulnerable customers should contact Russell Mackintosh (Synectics Head of Partnerships) in the first instance at email: Russell.Mackintosh@synectics-solutions.com or call: **0333 234 3414**.



DATA MARKETPLACE

IDENTIFY, AUTHENTICATE, AND MONITOR CUSTOMERS WITH CONFIDENCE WITH OUR DATA MARKETPLACE

The more clients know about their customers the better they can make accurate risk assessments about them.

Synectics Data Marketplace provides easy access to a wide variety of third-party intelligence sources, as well as our own proprietary intelligence, to enable the enrichment of your data to deliver more insight.

A NETWORK OF ESTABLISHED API'S FOR A RANGE OF GLOBAL INTELLIGENCE SOURCES

Access to an established range of plug'n'play APIs from a wide variety of leading global data providers enables our clients to switch on a multitude of data sources as the requirements of their risk or compliance analysis needs adapt over time.

OUR UNIQUE CONSORTIUM DATA SOURCES

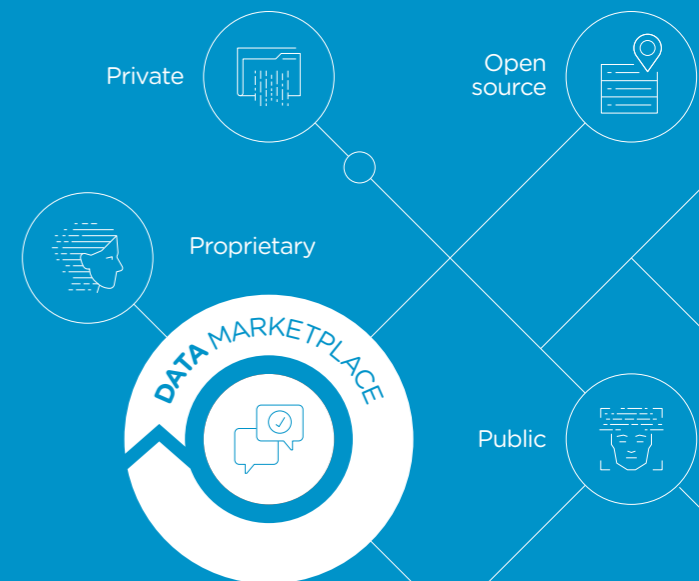
Uniquely, Synectics provides seamless access, through our platform, to two of the biggest public and private sector consortium fraud prevention databases - National SIRA and The National Fraud Initiative.

GET IN TOUCH WITH SYNECTICS TODAY

TO DISCUSS HOW WE CAN TRANSFORM YOUR ABILITY TO ASSESS YOUR CUSTOMERS FOR A MULTITUDE OF RISKS MORE EFFECTIVELY THAN EVER BEFORE.

CALL: **0333 234 3414**

OR EMAIL: INFO@SYNECTICS-SOLUTIONS.COM



Will our post-pandemic world stifle the transformation journey that many financial institutions have started ?



GARETH NARINESINGH, Commercial Director at Yoti, considers how UK banking is emerging from the pandemic and what will be the driving areas of adaptation required to remain competitive as the next few years unfold.

On a live event video webinar in August, the Governor of the Bank of England was asked whether he supported the use of digital identity in light of Covid. His response was "Absolutely!" He followed on by saying that in the event of an economic shock industry resilience was paramount, particularly for the fintech start-ups. He was concerned that a negative effect of a shock could dampen innovation and he did not want to see this impact on the digital economy.

Throughout the COVID-19 lockdown, it is true to say that UK financial services interest has peaked in electronic ID verification as a solution for remote customer onboarding.

"Challenger banks who have invested in technology and better customer experience flows are winning market share considerably..."

Yoti's measure of whether UK financial services can move towards more widespread adoption of digital identity is not actually based on escalating interest, it is more whether the sector's plans for digital transformation remain on track and how much progress is being made. The progress of a firm's digital transformation journey can be the determining or the inhibiting factor as to whether they can successfully deploy digital identity technology solutions.

In order to make it work, a firm must have in place even a basic IT platform which makes integration possible with electronic suppliers for things like data services, AML screening, application fraud checks or digital identity.

Consideration has to be given as to how to handle onboarding customers' personal information ("PI"). PI has to be handled securely and confidentially and needs to be routed through to the right places: core banking systems, compliance applications, customer relationship management tools and sales tracker databases. This requires a basic level of architectural sophistication and planning.

Also let's not forget that the customer journey also needs to be mapped out and understood, in order to provide a good experience such that drop off rates are not excessive. Challenger banks who have invested in technology and better customer experience flows are winning market share considerably over those who have either chosen not to invest to the extent required or delivered only partial digital transformation.

Although the fintechs have established themselves through use of digital identity as a customer acquisition tool, the FCA has unfortunately had to take regulatory action in several cases where onboarding protocols have fallen short of compliance expectations. It is therefore of critical importance to link electronic ID verification to the entire end-to-end KYC onboarding process for that customer. This means thinking about not just UX and customer flow but also linking this to quality and effective risk screening and risk assessment.

Platforms are being built today which deploy this comprehensive customer onboarding/compliance toolkit. One particular solution has recently come out of the FCA Sandbox this summer which gives full regulatory credibility to these types of tech solutions. One other solution coming to market as a pilot in the next couple of months will be the joint partnership platform provided by Yoti and Synectics.

We have decided to call our pilot Project Endeavour. This pilot promotes the use of portable, reusable digital identity as a concept, rather than one-time identity verification which is more common but requires the customer to prove themselves each and every time they make an application.

Endeavour will allow the customer to own their own KYC data as their PI and share it with whomever they choose. In this way, Project Endeavour will permit real-time onboarding for customers through the Yoti app, which is integrated into best-in-class data services and risk screening through the Synectics platform. A customer risk score can also be yielded which is beneficial to the receiving financial institution.

"...[it] requires the customer to prove themselves each and every time they make an application."

Yoti absolutely sees consumers and firms adopting these solutions over the next 3 years and it will become the norm for customers to hold a KYC credential within their digital identity wallet as an app on their mobile device. It benefits the consumer to own their own data and to be able to re-share their PI to get an automated decision.

Eventually the UK will allow the use of this kind of tech to allow consumers access to all kinds of products, services and even for air travel and border control. But as a first step, UK firms need to be bold, innovative and invest in their IT platforms so they can pilot, adopt and deploy these tech solutions



KNOW YOUR CUSTOMERS AND UNDERSTAND THEIR RISKS

CONTINUOUS, AUTOMATED CUSTOMER DUE DILIGENCE AND KYC MONITORING TO HELP REDUCE RISK, LOWER COSTS AND SAVE TIME

Sonar allows organisations to manage and automate the on-going monitoring of customer risk in real-time much more effectively and offers a host of benefits, including;



Reduce costs by removing the need for the manual remediation of customer portfolios



Faster more efficient KYC processing



Removal of siloed working to create a universal lens across the organisation for risk assessment



Improve your ability to target application treatment strategies more appropriately



Avoid fines and prosecutions from non-compliance with financial regulation



Improved customer boarding experience for 'green-lit' customers

GET IN TOUCH WITH SYNECTICS TODAY

TO DISCUSS HOW WE CAN TRANSFORM YOUR ABILITY TO ASSESS YOUR CUSTOMERS FOR A MULTITUDE OF RISKS MORE EFFECTIVELY THAN EVER BEFORE.

CALL:
0333 234 3414

OR EMAIL:
INFO@SYNECTICS-SOLUTIONS.COM



Are we paying enough

ATTENTION

to how fraudsters and cyber-criminals are adapting their fraud tactics to the post COVID-19 world?

IS ENOUGH THOUGHT INVESTED IN TRYING TO DISCOVER WHAT THESE GROUPS ARE UP TO?

As an expert in fraud and cybercrime, Peter Taylor has over 20 years' experience working both within the UK Police Force and independently as a private investigator. In this article, he shares some insight into his recent research amongst criminal groups he has access to from his research and connections.

In 2020 everything changed because of the COVID-19 Pandemic. What initially seemed to be happening to other people elsewhere, impacted globally and severely in the UK - with the UK government imposing an unprecedented lockdown on the public to prevent the NHS being overwhelmed. There was no pretence that the economy would not adversely suffer or a definitive duration for the lockdown.

The words 'uncharted territory' and 'unprecedented' became universal across government and business. There were various actions taken to support individuals and businesses. Whether we believe they were unnecessary, welcome, or not enough they meant that huge sums of taxpayers' money are being paid out through loans, grants, and furlough or to underwrite borrowing via the British Business Bank.

Whilst lockdown initially made life difficult for criminals, the climate of fear, financial uncertainty, urgency, and despair that was widespread throughout the UK's population eventually played into the hands of fraudsters and cyber criminals.

“ Now that we are begging to emerge from this initial period we need to take back control with some robust analysis and action and reflect on how those with criminal intent have exploited the situation.”

The government's rush to get money to people who needed it meant that many counter-fraud measures, and levels of due diligence, were understandably relaxed. This may have been a good thing as a temporary measure to ease the pain people were experiencing in the economy, but it has undoubtedly enabled more crime to take place. Now that we are begging to emerge from this initial period we need to take back control with some robust analysis and action and reflect on how those with criminal intent have exploited the situation.

We in the counter-fraud community predicted the key areas to alert government, business, and individuals about. These included fraudulent applications for the Bounce Back Loan Scheme (BBLS), COVID Business Interruption Loans (CBILS), Local Authority Grants, Furlough payments (while staff actually kept on working). We also correctly warned of increased Phishing activity to capitalise on people working remotely to compromise their devices and steal data.

“ To understand this, a better an understanding of the criminal mind would seem to be of some use. To do this, we need to actually go behind 'enemy lines' so to speak and see what's happening...”

Additionally, with financial uncertainty and people in the general population becoming more financially vulnerable or desperate there was also the concern that people of good character would be much more willing to become involved in fraud - or at least ask less questions when asked to take payments into their bank accounts. Sadly it would appear that all of these have come to fruition.

To understand this, a better an understanding of the criminal mind would seem to be of some use. To do this, we need to actually go behind 'enemy lines' so to speak and see what's happening - and what is the perspective from the fraudster/cybercrime community.

As a specialist in threats from fraud and organised cybercrime, I have looked into fraud within COVID-19 related areas, initially by looking at what was happening in countries in the vanguard of the pandemic, such as Italy, to understand what had happened there from a financial crime perspective.



Accounts from Italy began to emerge back in March 2020 of crime gangs approaching businesses that were struggling because of COVID-19 and making them an offer to buy their business. When a price was agreed the criminals were then able to use an established business to launder money and exploit it as a conduit to process receipts from other criminal activities. We have seen similar activities like this in the UK where not only are 'acquired' businesses used to launder money, but are also being encouraged by criminal elements to apply for fraudulent grants, BBLS, CBILS, etc.

“ Unsurprisingly, the UK and USA cyber criminals are all describing government COVID-19 loans/grants as 'free money' ...”

To qualify for the COVID-19 loans/grants businesses in the UK must have been established before 1st March 2020. We now see Limited Companies with little or no trading history being advertised for sale on sites like eBay for thousands of pounds. The adverts often feature the date the company was registered (with dates like 2018 being favoured). In amongst the advertisements are the ominous words 'never applied for a BBLS'. Whilst the seller may not be committing any fraud directly, these companies have become very attractive to the fraudsters.

While writing this article, I spoke with a UK Police contact who informed me that they are aware of this issue, and one of the checks they now run is whether a company has a new Director, appointed within the last few months, and particularly where that person is making all the applications for COVID related loans etc.

The true impact of BBLS/CBILS fraud will not be seen until 2021 (or even later) when the loans become due and payments are needed. I think it's safe to say that we can certainly expect to see a wave of defaults, businesses that have closed, and directors that can no longer be found.

Recently, I have also spent some time researching the 'Dark Web' and criminal activity there, to see what's changed during this pandemic. Unsurprisingly, the UK and USA cyber criminals are all describing government COVID-19 loans/grants as 'free money' - and planning to get their hands on as much of it as possible.

Not only are these organisations attempting to put in falsified applications for this support, but also target those businesses who haven't claimed grants and loans, and then claiming fraudulently on their behalf. They are also ramping up their use of false identities to make unemployment claims. In fact, the USA Secret Service has recently alerted us about organised scams claiming millions in unemployment benefits across various States - and even named a specific cybercrime gang, called Scattered Canary, as being one known such 'gang' behind it.

My sources also inform me that these gangs are currently making so much money that they don't currently have sufficient infrastructure to launder or 'cash out' their gains. There is therefore hope yet that some of these losses can be recuperated by law enforcement before it's too late. I know from my own previous research that 'cashing out' is one of the biggest obstacles that gangs face when they have generated illegal income. So recently acquired 'legitimate' businesses and intricate use of various forms of cryptocurrencies are all areas being considered by these types of organisations as a route to transfer their gains and get them into the legitimate financial world.

With remote working having become the norm, 'Business Email Compromise' has also reportedly grown considerably. There has been a blaze of media coverage that COVID-19 headlines are being used in scam emails to target victims to open emails and download malware or provide information. Finding victims for this type of scam is a numbers game with high volumes of emails being sent out. When researching the issue with my contacts, I was told that rather than it being new players getting into this market, existing groups have revisited this 'business channel' because by using COVID within the emails or texts they are now getting four times as many people responding.

Finally, when it comes to identity fraud, many fraudsters have been well aware of various tech companies developing solutions to address ID fraud and have been busy pre-preparing and using synthetic identities for use in fraud over the past 3 years. However, because of opportunities with grants, loans, and unemployment benefit many have kept to using genuine identities over the last few months - and amended information attached to that identity to meet eligibility criteria. Failing that, just the ability to apply pressure to vulnerable people during a crisis (whether they be in struggling businesses or just vulnerable circumstances) is providing lots of opportunity for them during this health emergency.

“ Usually, you have desperate criminals trying to steal good people's money. Now the good people are desperate too, so they are easier to exploit and harder to spot.”

My view, however, is that as the COVID-specific fraud opportunities subside, rather than sit back and enjoy their spoils, these criminals will seek to maintain their level of activity and these pre-prepared synthetic identities will be a vital part of that - as they seek to circumvent the various tech solutions being considered to address identity fraud.

As a final comment, I asked Brett Johnson, a reformed cyber criminal, how he would describe COVID-19's impact on fraud. He said 'Usually, you have desperate criminals trying to steal good people's money. Now the good people are desperate too, so they are easier to exploit and harder to spot.'

Links for sources
<https://www.bbc.co.uk/news/world-europe-52537573>

Mafia and COVID-19
<https://www.wired.com/story/nigerian-scammers-unemployment-system-scattered-canary/>

US Payments

HAS APP FRAUD AND PAYEE AUTHENTICATION BECOME ONE OF THE MOST PRESSING CHALLENGES IN 2020 FOR FRAUD TEAMS?



Despite all kinds of fraud and financial crime being a consistently growing issue, one particular type of fraud stands out currently as the issue for many in the UK banking industry. Authorised Push Payment (APP) scams and 3rd party payment fraud have become one of these most pressing issues to address in 2020.

IS THERE A SOLUTION TO THE PROBLEM OF APP FRAUD AND PAYEE AUTHENTICATION?

Understandably there is a lot of effort going on across the industry to try and create a framework or set of tools that will help to prevent or at least mitigate this issue.

The reason that this issue has rapidly risen to the top of the agenda is down to a number of factors, the main one being the publication of the Authorised Push Payment Contingent Reimbursement Model (APP CRM) as a voluntary code of practice - which is being adopted by a large swathe of the banking sector in the hope of avoiding the need for FCA regulation.

Additionally, media, customer and regulatory pressures have also raised the profile of this problem, such that it has risen on the agenda of things that need to have some kind of industry wide consensus for solving.

In fact, when one looks at the losses incurred in recent times by APP scams, in 2019 the industry saw a staggering £450million of APP fraud. Within that figure, a recent report by UK Finance last year also confirmed that £101.1m fell within the remit of the APP CRM, and of this £41.3m was refunded under the code to customers where the Banks were deemed liable.

£450 MILLION

IN APP FRAUD WHERE BANKS WERE DEEMED LIABLE FOR £41.3 MILLION



Given the difficulty in spotting these type of scams, financial criminals have been quick to spot this opportunity, which has meant that this type of fraud has seen significant growth in recent years and unless banks can find better ways to address it the likelihood is it will grow exponentially as an issue. In fact, in 2019 there was a massive 29% growth in APP fraud, when compared to 2018.

Obviously, prior to 2019 the burden of this type of fraud was being borne by the customers, but now with the introduction of APP CRM, the industry is

starting to commit to customers being refunded for these APP scam payments, which ultimately leaves banks and other financial institutions liable for the losses.

A deeper look at the model of an APP scam helps us to understand why it's such a difficult problem to spot and prevent.

When a customer is being socially engineered for the purpose of (APP) Scams because genuine customers are merely accessing their own accounts and passing payments to 3rd parties, at the point of inception of the crime, it is pretty much impossible for a Bank to detect the issue of the APP scam taking place. Resulting in an APP claim being received at a later date which banks are now increasingly liable for.

The sophisticated techniques that are employed to socially engineer customers means that no matter how much awareness raising banks try to do they struggle to break the spell which has been cast over the customer by the scammer. This can often be seen in the high-value losses the industry is experiencing despite expensive awareness campaigns directed at customers.

Recent anecdotal research from Synectics in this area also points to the fact that the COVID-19 pandemic has only exacerbated this issue. APP scammers are feeding off the vulnerability and confusion that the pandemic has created. One recent example of this is as follows:

A Purchase scam - where a scammer has posed as a supplier of face masks. The customer is asked to send the money via an APP to purchase a bulk delivery, as the customer is looking to sell on the product for a profit. However, the face masks never existed and once the customer has sent the funds, the scammer disappears and the customer is left without the product or the money.

DELAYING FASTER PAYMENTS

One of the first initiatives to be adopted by banks was to delay the actual transfer for 'first time payee' transfers by 24 hrs to at least give customers a brief period of time to assess if they have been scammed. While this helps, obviously in the vast majority of cases in can be days or weeks before a scam becomes apparent and so this, while welcome, has never been seen to be the solution.

PAY.UK AND CONFORMATION OF PAYEE - COP

Pay.uk, the UK's retail payments authority have created a system called Confirmation of Payee (CoP). This allows the sender of funds from one account to another to check the name on the receiving account, making sure it matches with the name they would expect. Although this has been welcomed by the industry, the feeling is that this is one safety net that sophisticated criminals will be able to circumvent fairly easily before too long.

Synectics is currently working with a range of intelligence providers and adapting its Data Marketplace as part of its research into delivering the necessary intelligence and syndicated trust framework that could provide such a solution to help banks with APP and Payee Authentication.

IDENTIFYING VULNERABLE DEMOGRAPHICS AND PUTTING ENHANCED PAYEE DUE DILIGENCE IN PLACE

Given that certain demographics of customer seem to be more prone to falling victim to APP scams, such as the elderly or those suffering with certain health issues, one possible method would be to put greater due diligence around payments and transfers from customers who fall into these risk categories.

Synectics is currently working with the Vulnerability Registration Service on helping those who self-identify as being in a vulnerable group and can then notify banks and other financial institutions of this status. It's early days yet but this type of shared intelligence could become part of a useful set of 'risk flags' that would help banks with their APP due-diligence.

CREATING A 'TRUST SCORE' FOR APP-PAYEE RISK ASSESSMENT/ AUTHENTICATION IS THE ULTIMATE SOLUTION

To deliver a much more thorough resolution to combat the issue of APP fraud, and provide the kind of payee authentication that will really address the issue, we at Synectics think what is really required is a solution that allows a bank processing payments to be in a position to properly risk assess a variety of data points for the recipient account of any payment.

By providing a bank issuing payments with the ability to obtain immediate intelligence on a range of recipient account details, in real-time, prior to transferring funds they will be able to complete a thorough, holistic risk review of the payment prior to transfer of funds.

Furthermore, by building up a syndicated intelligence resource of both trusted and 'adverse' payment profiles a trust model could be derived that associates a payee authentication trust score against different combinations of markers.

Ultimately, this will allow the issuing bank to complete a fast and holistic review of the transaction which is being processed, when coupling the trust score and any other internal risk markers that are created through the customers logon journey.

Banks or any other financial institutions interested in having a deeper conversation on our research and development in this area should get in touch with our Product Development team and, either email Anthony Minshull Anthony.Minshull@synectics-solutions.com or call **03333 234 3414**

UPCOMING EVENTS

Being part of Synectics Solutions shared ecosystem for financial crime intelligence means building on the shared knowledge that your peers can provide to help evolve your fraud strategies.

The following thematic calls, events and webinars are coming in later this year for you to pop in your diary.



SYNECTICS THEMATIC CALLS

ONLY AVAILABLE TO MEMBERS OF NATIONAL SIRA

HOW THEY WORK

Once you receive the invite, join the call at the specified time and date. You will be asked if you have anything to contribute and will also be able to discuss trends/best practice with other SIRA members.

COME PREPARED

These calls are about sharing intel, fraud trends and best practice.

SHARE BEST PRACTICE

The benefit from attending the calls is sharing best practice with other SIRA members.

THEMATIC CALL DATES

INSURANCE

Focus on Claims Fraud
14th October 2020

Focus on Policy Fraud
25th November 2020

Focus on Claims Fraud
16th December 2020



FINANCE

Focus on 'Non-Mortgage' Fraud
15th October 2020

Focus on Motor Finance Fraud
5th November 2020

Focus on Mortgage' Fraud
26th November 2020

Focus on 'Non-Mortgage' Fraud
17th December 2020



ECONOMIC CRIME ACADEMY WEBINARS IN ASSOCIATION WITH UK FINANCE



UK FINANCE

For the last 3 years, Synectics has been working with UK Finance to run the UK Economic Crime Academy webinar programme to bring together key figures in the UK's financial services market to discuss solutions to some of the industry's biggest economic crime challenges.

Visit: www.ukfinance.org.uk/events-training/webinars to register your interest in attending these webinars.

OCTOBER 7TH 2020

Addressing the issue of APP fraud and improving methods of Payee Authentication

APP fraud and Payee Authentication have become two of the most intractable issues for fraud prevention teams across the UK in recent times. Since the publication of the Authorised Push Payment Contingent Reimbursement Model (APP CRM) in 2019 banks have also had to take on much more liability for the losses that APP scams have generated – which was an estimated £450 Million in 2019. On this webinar, Anthony Minshull from Synectics Solutions will be joining UK Finance to understand some of the latest thinking in how to address the challenges that APP fraud scams pose for banks and other financial institutions. In addition to that, we will be exploring the various opportunities that exist to use technology or increased intelligence sharing to create a Payee Authentication Trust Framework that would allow banks to be far more effective at assessing the risk of digital payment transfers before they take place.

ECONOMIC CRIME ACADEMY WEBINARS COMING UP IN 2021

During 2021 we are looking forward to publishing the following webinars designed to explore solutions to some of the most challenging aspects of economic crime for UK financial institutions.

Assessing the issues that COVID19 will have on economic crime and identifying solutions to address the major impacts

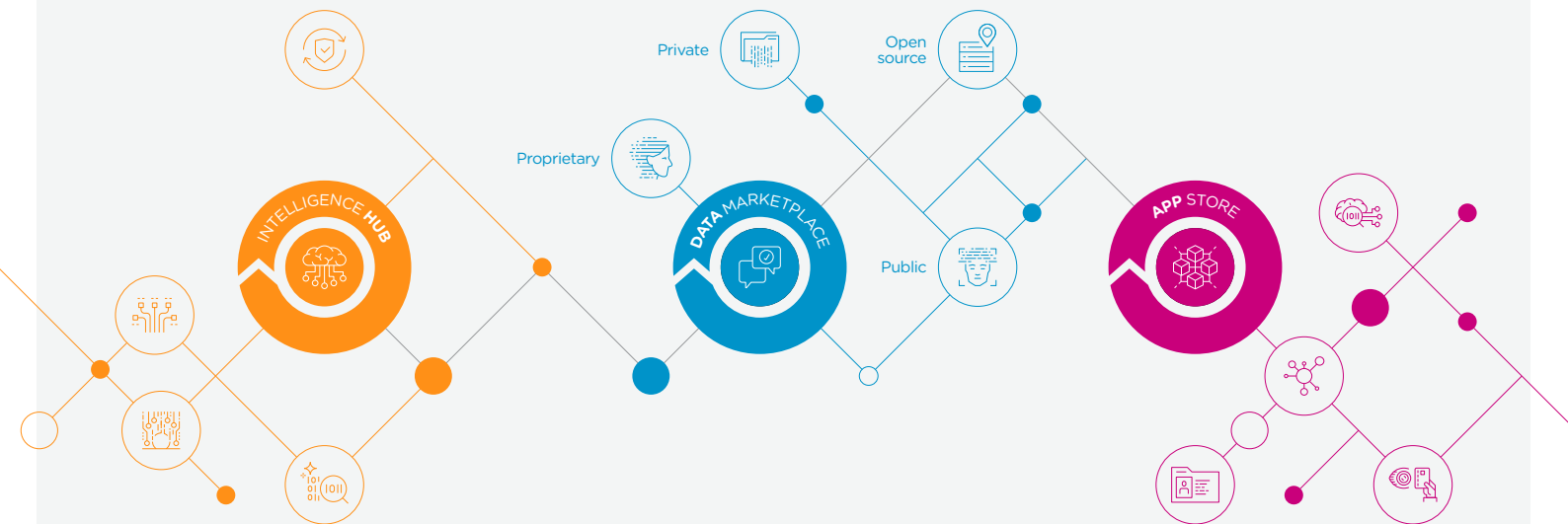
Creating a more effective CBIL/BBLs recovery strategy through public/private sector intelligence sharing

Creating a cost-effective, friction-right, customer on-boarding process for banking

Finding an acceptable consensus on how Digital Identity will work in UK banking

TRANSFORM YOUR APPROACH TO REGULATORY RISK MANAGEMENT, FINANCIAL CRIME AND FRAUD PREVENTION

Synectics Financial Crime Risk Management platform will enable you to transform your approach to a range of compliance, financial crime and fraud prevention challenges. By deploying our unified, organisation-wide solution, the Synectics FCRM platform will transform your ability to create the kind of automated, real-time, customer-decisioning capabilities that a modern financial services brand needs to be competitive in today's turbulent markets.



ACCELERATE YOUR CUSTOMER ON-BOARDING PROCESS

Meet the fast boarding process that your customers demand without compromising on the range and sophistication of your fraud and financial crime risk analysis. Needs to remain competitive in this turbulent market place.

ALIGN FINANCIAL CRIME DEFENCE WITH YOUR COMMERCIAL BUSINESS OBJECTIVES

Reduce siloed working and adapt to changes in both regulation and financial crime risks across your organisation without compromising your ability to get products to market.

REDUCE THE COST OF REGULATORY COMPLIANCE

Comply with key regulations such as 5MLD & PSD2 and create effective treatment strategies to improve customer relationships and reduce costs through continually monitoring customers.

TO DISCUSS HOW OUR FCRM PLATFORM COULD TRANSFORM YOUR ABILITY TO CREATE A SEAMLESS DIGITAL CUSTOMER BOARDING SOLUTION WITHOUT COMPROMISING ON YOUR RISK OR DUE-DILIGENCE CHECKS

CALL: 0333 234 3414 OR EMAIL: INFO@SYNECTICS-SOLUTIONS.COM



Synectics Solutions Ltd, Synectics House, The Brampton
Newcastle-under-Lyme, Staffordshire, ST5 0QY

+44 (0)333 234 3414
info@synectics-solutions.com
www.synectics-solutions.com

Synectics Solutions

@Syn_Sol

Synectics Solutions

